Bond Case Briefs

Municipal Finance Law Since 1971

How Local Governments Are Handling a Threat They Can't See.

The proliferation of cyberattacks has prompted Pennsylvania municipalities to take extra steps to secure their systems. Here's what they're doing.

In 2018, an Allentown city employee took a city laptop with him on a work trip. During that trip, he opened a phishing email that ultimately cost the city more than $1 million in repairs to its digital infrastructure. Hackers, based in Ukraine, hit the Lehigh Valley city with malware known as Emotet—which the federal Cybersecurity & Infrastructure Security Agency ominously describes as "an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload"—that began to self-replicate, steal credentials and work its way across their computer systems.

"A colleague came down the hall and said, 'Hey, my account's locked'—and I went to sign in and found that my account was locked" as well, Matthew Leibert, Allentown's longtime chief information officer, recalled of the moment he knew something was seriously wrong—a realization that hit him physically as well. "I definitely felt sick," he added.

Four years—and millions of dollars of sunk costs later—his staff still struggles to keep up with the monitoring and maintenance required to keep their systems safe for this city of more than 120,000 residents.

Continue reading.

Route Fifty

By Harrison Cann

JULY 28, 2022